EXHIBIT A

RETURN DATE: JUNE 4, 2019

ARYEH SIMON AND SASSYA SIMON, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED, Plaintiffs, **v.** **MARRIOTT INTERNATIONAL, INC., STARWOOD HOTELS & RESORTS WORLDWIDE LLC, ARNE SORENSON, AND DOES 1-5,** Defendants.	**SUPERIOR COURT** **JUDICIAL DISTRICT OF STAMFORD** **AT STAMFORD** **MAY 7, 2019**

CLASS ACTION COMPLAINT

Plaintiffs Aryeh and Sassya Simon, on behalf of themselves and all others similarly situated, allege as follows against Defendants Marriott International, Inc. ("Marriott"), Starwood Hotels & Resorts Worldwide LLC ("Starwood"), Arne M. Sorenson ("Sorenson") as President and Chief Executive Officer of Marriott, and Does 1-5.

SUMMARY OF THE CASE

1. On November 30, 2018, Marriott announced a "data security incident" involving "unauthorized access to the Starwood network since 2014" (the "Data Breach"). The Data Breach, by Defendants' own admission, exposed information relating to hundreds of millions of people worldwide. Marriott initially estimated that "approximately 500 million guests" had their information exposed in the Data Breach, but "after further data analysis" lowered their estimate to 383 million "guest records."

2. The types of information exposed in the Data Breach (collectively, "Personal Information") include, but are not limited to: names, mailing addresses, telephone numbers, email addresses, passport numbers, birth dates, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, and payment card expiration dates.

3. Defendants knew that they had an obligation to protect Personal Information, but failed to use reasonable measures to do so. Defendants left Personal Information unencrypted, improperly handled and stored it, and failed to maintain it in accordance with applicable cyber-security policies and procedures. Due to these failures, hackers were able to access Personal Information during a period extending from 2014 through at least September 2018.

4. Defendants failed to disclose to individuals whose Personal Information was stored in Starwood's reservation systems and databases – including travelers who booked reservations through the Starwood reservation system or who were members of Starwood's Preferred Guest ("SPG") loyalty program – that their Personal Information was at risk.

5. Defendants also failed to provide timely, accurate, and adequate notice of the Data Breach to Plaintiffs or to the hundreds of millions of other individuals who had their data compromised in the Data Breach.

6. Due to Defendants' failures, Plaintiffs and others like them have had their Personal Information exposed to malicious actors. Their Personal Information – the protection of which they relied on as part of the "benefit of the bargain" for doing business with Starwood or Marriott – is now, as a result of the Data Breach,

available on the "Dark Web," allowing fraudsters to obtain the information they need to commit identity theft and other crimes. As a consequence, Plaintiffs and others like them have been harmed and suffered damages.

7. After the Data Breach, Plaintiffs have each received notice from a commercial monitoring service that their Personal Information is available on the Dark Web. Plaintiffs have no reason to believe that their information was leaked to the Dark Web through any avenue other than the Data Breach.

8. Accordingly, on behalf of themselves and those similarly situated, Plaintiffs seek damages, as well as injunctive relief to ensure that Marriott adequately protects Personal Information going forward.

JURISDICTION AND VENUE

9. Defendants intentionally avail themselves of this jurisdiction by conducting Starwood's corporate operations here and by promoting, selling, and marketing Starwood's and Marriott's services within Connecticut. Defendant Starwood maintains its principal headquarters at One StarPoint (formerly 333 Ludlow Street), Stamford, Connecticut 06902.

10. A federal court would lack subject-matter jurisdiction over this action. The plaintiffs are American citizens domiciled abroad and thus are not citizens of any U.S. state for purposes of 28 U.S.C. § 1332.

11. Venue is proper because Marriott and Starwood are corporations that regularly conduct business in this judicial district, including the business conducted at Starwood's headquarters. Venue is also proper because a substantial number of the events or omissions giving rise to the claims in this action occurred in or

emanated from this district, including the decisions made by Starwood's governance and management personnel that led to and perpetuated the Data Breach.

PARTIES

12. Plaintiffs Aryeh Simon and Sassya Simon, who are married to each other, are each citizens of both the United States and Israel who are domiciled in Israel. The Simons made Israel their permanent home in 2007 and have lived there ever since. Both "made Aliyah," *i.e.*, both emigrated to Israel under the Law of Return 1950, returning to Israel to make it their home. The couple owns their home in Israel, and their children attend school nearby. They work and are licensed to drive in Israel. The Simons own no residences outside of Israel, and they have no intention of moving outside of Israel.

13. Plaintiffs have each stayed at Marriott and/or Starwood hotels during the Relevant Period. In addition, Plaintiff Aryeh Simon has been a member of Starwood's SPG loyalty program since 2007. Plaintiffs each provided Personal Information to Defendants on the understanding that Defendants would keep it secure, employ reasonable and adequate security measures to ensure that hackers would not compromise it, and notify them promptly in the event of a breach.

14. Defendant Marriott International, Inc., is a Delaware corporation with its principal executive offices located at 10400 Fernwood Road, Bethesda, Maryland 20817.

15. Defendant Starwood Hotels & Resorts Worldwide LLC is an indirect, wholly owned subsidiary of Marriott. On September 23, 2016, Marriott acquired Starwood, formerly known as Starwood Hotels & Resorts Worldwide, Inc. Starwood's principal

executive offices are, and at all relevant times were, located at One StarPoint (formerly, 333 Ludlow Street), Stamford, Connecticut 06902.

16. Defendant Arne M. Sorenson has served as Marriott's President and Chief Executive Officer since March 31, 2012. Defendant Sorenson was directly involved in the management of Marriott and exercised control over Starwood and Marriott. Sorenson was directly or indirectly involved in the oversight or implementation of Marriott's internal controls regarding the privacy of Starwood and Marriott guests.

17. The true names of Does 1 through 5 ("Doe Defendants"), whether individual, corporate, associate, or otherwise, are unknown to Plaintiffs, who sue these Defendants under fictitious names. Each of the Doe Defendants is responsible in some manner for the conduct alleged herein, including, without limitation, by way of aiding, abetting, furnishing the means for, and/or acting in capacities that create agency, *respondeat superior*, and/or predecessor or successor-in-interest relationships with other Defendants. The Doe Defendants actively assisted or participated in the negligent and wrongful conduct alleged herein in ways that are currently unknown to Plaintiffs.

18. Plaintiffs make all allegations contained in this Complaint against all Defendants, including the Doe Defendants. Plaintiffs reserve the right to amend this Complaint to allege the true names, capacities, and actions of the Doe Defendants once they are ascertained, and to add additional facts and/or legal theories.

FACTUAL BACKGROUND

A. Starwood and Marriott Collect and Store Personal Information

19. Marriott is a global hospitality company that operates more than 6,700 properties in 130 countries and territories. Marriott reported $22 billion in revenue in 2017.

20. In November 2015, Marriott announced that it would purchase Starwood for $13.6 billion. Marriott's acquisition of Starwood was completed in September 2016, making Marriott the world's largest hotel chain. Before the acquisition, Starwood was a separate hospitality company that operated hotel brands including W Hotels, St. Regis, Sheraton, Four Points by Sheraton, Westin, Element, Aloft, The Luxury Collection, Tribute Portfolio, Le Meridien, and Design Hotels, as well as Starwood-branded timeshare properties.

21. Starwood's reservation system was purportedly separate from pre-acquisition Marriott hotels' reservation systems until at least December 2018.

22. At all times relevant to this action, Starwood and Marriott received and stored massive amounts of Personal Information and used that information to maximize profits through predictive marketing and other marketing techniques. Starwood and Marriott promised to maintain this Personal Information in accordance with their privacy policies.

23. Plaintiffs would not have obtained SPG membership, stayed at a Starwood or Marriott property, or supplied their Personal Information for reservations had they known that Defendants would not adequately protect their Personal

Information. Alternatively, even if Plaintiffs had known the concealed risk inherent in booking at Starwood or Marriott properties and chosen to book anyway, the room would have been worth less in the marketplace, in order to compensate them for that risk.

24. Starwood and Marriott failed to disclose their negligent and insufficient data security practices, including the unencrypted storage of payment card information and passport numbers. Plaintiffs and consumers relied on or were misled by these omissions when they made reservations and supplied Personal Information to Starwood or Marriott through their SPG membership or otherwise.

25. By withholding important information from consumers about Starwood's and Marriott's data security, Defendants created an asymmetry of information between themselves and consumers that precluded consumers from acting to avoid or mitigate injury.

B. Personal Information Has Significant Value and Must Be Protected

26. Defendants knew or should have known at all relevant times that Personal Information is valuable and a frequent target of hackers and other malicious actors. The names, email addresses, telephone numbers, payment and passport card, and other Personal Information provided to Starwood and Marriott can be used to gain access to a variety of consumer accounts and websites.

27. The value of Personal Information on the black market is widely known. For example, the Federal Trade Commission sued Wyndham Worldwide Corporation in 2012 because the company failed to provide reasonable cybersecurity

protections for customer data. In August 2018, the U.S. Department of Justice indicted members of an Eastern European cybercrime ring called Fin7, which targeted, among others, hotel chains. Despite this well-publicized litigation and the frequent public announcements of data breaches by retailers and hotel chains, Defendants chose to maintain an inadequate system to protect the Personal Information of Plaintiffs and other class members.

28. Once stolen, Personal Information can be used in different ways. One of the most common uses is to offer the Personal Information for sale on the Dark Web, an opaque part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The Dark Web is not indexed by normal search engines such as Google and is only accessible using a specialized tool that aims to conceal users' identities and online activity. When Personal Information ends up on the Dark Web, there is almost no way to track down who has gained access to that Personal Information.

29. Once someone buys Personal Information, the buyer can then use it to infiltrate different areas of that person's digital life, including bank accounts, social media accounts, and credit card accounts. By breaking into the victim's accounts, a buyer can obtain even more sensitive data from those accounts.

30. Identity thieves can also use stolen Personal Information to embarrass, blackmail, or harass, or to commit fraud, including by fraudulently obtaining identification documents, tax refunds, and government benefits. Victims of "new account identity theft" – *i.e.*, the opening of new credit or other accounts using stolen personal information – must correct fraudulent information in their credit

reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with creditors. Many of these measures require victims to incur expenses.

31. Another form of identity theft, dubbed "synthetic identity theft," occurs when thieves combine real and fake identifying information to create new identities, then use those identities to open new accounts. Synthetic identity theft is more difficult to unravel than traditional identity theft because it is not tied to a single individual.

32. The problems associated with the theft of Personal Information are made worse by the fact that many identity thieves wait years before attempting to use the Personal Information they have obtained. To protect themselves, victims need to remain vigilant against unauthorized data use for years or even decades.

C. Defendants' Inadequate Data Security Allowed the Breach of Hundreds of Millions of Individuals' Records

33. On November 30, 2018, Marriott first announced the Data Breach, estimating that the Personal Information of 500 million consumers had been affected.

34. Marriott claimed that it discovered the vulnerability on September 8, 2018 "from an internal security tool regarding an attempt to access the Starwood guest reservation database," and that it "engaged leading security experts to help determine what occurred."

35. Marriott reported that unauthorized actors had copied and encrypted information and had attempted to "remove" or, in other words, exfiltrate that Personal Information.

36. Marriott later determined that the contents were from its Starwood guest reservation database.

37. Marriott admitted that unauthorized actors had had access to the Starwood guest reservation database since 2014.

38. The Starwood guest reservation database contains guests' and potential guests' Personal Information, including names, addresses, phone numbers, email addresses, passport numbers, SPG account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, and payment card expiration dates.

39. The Data Breach is among the largest breaches in U.S. history. Marriott has disclosed that as many as 383 million records were stolen, including 5.25 million unencrypted passport numbers, 18.5 million encrypted passport numbers, and 9.1 million payment card numbers.

40. Asked in December 2018 how Marriott was handling guest and potential guest information since it merged Starwood's data into the Marriott reservations system, a company spokesperson stated, as reported in the New York Times: "We are looking into our ability to move to universal encryption of passport numbers and will be working with our systems vendors to better understand their capabilities, as well as reviewing applicable national and local regulations."

41. Defendants' storage of unencrypted passport and payment card data was extremely reckless and unsafe. So was their treatment of encrypted data. Indeed, Defendants used only AES-128 encryption, which required only two elements for decryption, both of which appear to have been compromised in the Data Breach.

42. The Data Breach affected individuals all over the world. Marriott set up dedicated call centers to deal with the Data Breach in at least 55 countries, including Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Chile, China, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong SAR, China, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, the Netherlands, New Zealand, Peru, Philippines, Poland, Portugal, Romania, Russia, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, United Arab Emirates, the United Kingdom, the United States, and Vietnam.

43. Marriott had reason to be especially vigilant regarding cyber-security. In 2015, right after Marriott announced that it was acquiring Starwood, Starwood reported a data breach affecting hotel guests at many properties that occurred between November 2014 and October 2015. Considering that breach, Marriott knowingly accepted considerable risk by acquiring Starwood, and it should have been on alert for other infirmities in Starwood's cyber-security.

44. Quoted in the New York Times, the executive director of Privacy International was incredulous that it purportedly took Defendants four years to detect the Data Breach:

> It's astonishing how long it took them to discover they were breached. For four years, data was being pilfered out of the company and they didn't notice. They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing.

D. Defendants Failed to Comply with FTC Requirements

45. Federal and state governments have established security standards and issued recommendations to deter and prevent data breaches and the resulting harm to consumers. The Federal Trade Commission ("FTC") has issued numerous guides highlighting the importance of reasonable data security practices.

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices. The guidelines state that businesses should protect the Personal Information that they keep, properly dispose of Personal Information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicative of hacking attempts, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies: (i) not maintain cardholder information for longer than is needed for authorization of a transaction; (ii) limit access to sensitive data; (iii) require complex passwords to be used on networks; (iv) use industry-tested methods for security; (v) monitor for suspicious activity on the network; and (vi) verify that third-party service providers have implemented reasonable security measures.

48. At all relevant times, Defendants were fully aware of their obligation to protect the Personal Information of Starwood's and Marriott's guests, users, and

customers. Defendants also were aware of the significant repercussions of failing to protect Personal Information. Starwood and Marriott collected Personal Information from hundreds of millions of guests and consumers and knew that failing to protect this data would result in injury to consumers.

49. Despite understanding the consequences of inadequate data security, Defendants failed to take appropriate protective measures to secure the Personal Information of guests and other individuals, including Plaintiffs and class members.

50. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act").

E. Defendants' Inadequate Post-Data Breach Response

51. Defendants delayed notifying Plaintiffs and class members of the Data Breach for at least three months, from September to November 2018. The delay may have been much longer, as Marriott's due diligence in acquiring Starwood should have, and may indeed have, uncovered the Data Breach long before September 2018.

52. On November 30, 2018, Marriott issued a press release announcing the Data Breach for the first time. The press release stated that Personal Information which was compromised included names, mailing addresses, telephone numbers, email addresses, passport numbers, birth dates, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, and payment card expiration dates. According to the press release, Marriott was

first alerted to the Data Breach on September 8, 2018 via an "internal security tool, and that the company had more recently "discovered that an authorized party had copied and encrypted information, and took steps toward removing it." It quotes Defendant CEO Sorenson as stating "[w]e deeply regret this incident happened," that "[w]e fell short of what our guests deserve and what we expect of ourselves." The press release informed consumers that the company would "send[] emails ... to affected guests" and that it would provide guests the opportunity to enroll in a service that "monitors internet sites where personal information is shared" (*i.e.* the Dark Web) "free of charge for one year."

53. Because of the delay in notifying consumers of their potential exposure, Plaintiffs and other class members face a heightened risk of fraud than they otherwise would have had Defendants timely disclosed the Data Breach.

54. Both because of (i) the delay in notification and (ii) the absence of sufficiently detailed information in the belated disclosures Marriott did make, Plaintiffs and class members were left exposed to continued misuse, and an ongoing risk of misuse, of their Personal Information.

F. Plaintiffs and Class Members Were Injured And Suffered Damages

55. Plaintiff Aryeh Simon has been a member of the SPG loyalty program since 2007. In addition, during the period of the Data Breach, Plaintiffs were guests at multiple Starwood properties in Israel and Canada. As a necessary consequence of their transactions and interactions with Starwood and Marriott, Plaintiffs provided Personal Information to Defendants.

56. Since Marriott announced the Data Breach, Plaintiffs have each separately received an email from Marriott indicating that their Personal Information was exposed in the Data Breach. In addition, each Plaintiff has received a "dark web alert" from a commercial monitoring service that their Personal Information has been "compromised" as of at least July 2018. Plaintiffs believe, and have no reason not to believe, that their information was leaked to the Dark Web via the Data Breach.

57. The Personal Information of Plaintiffs and class members is private and sensitive, and Defendants did not adequately protect it. Starwood and Marriott were not authorized to disclose Plaintiffs' and class members' Personal Information.

58. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and class members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law. This includes Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and class members' Personal Information, and their failure to protect against reasonably foreseeable threats to the security of such information.

59. Starwood and Marriott had the resources to prevent or timely detect a breach. They made significant expenditures to market their hotels and hospitality services, but neglected to adequately invest in data security, despite the growing number of data intrusions and several years of well-publicized data breaches.

60. Had Defendants remedied the deficiencies in Starwood's and Marriott's information storage and security systems, followed industry guidelines, and adopted

security measures recommended as minimum requirements by experts in the field, they would have prevented or timely detected intrusion into their systems and the theft of Plaintiff's and class members' Personal Information.

61. As a direct and proximate result of Defendants' wrongful actions and inactions and the resulting Data Breach, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and make the effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely monitoring their credit reports and accounts for unauthorized activity.

62. Defendants' wrongful actions and inactions directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and class members' Personal Information, causing Plaintiffs and class members to suffer, and continue to suffer, compensable economic damages and other actual harm stemming from, for example:

a. theft of their personal, financial, and identity information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and misused via the sale of Plaintiffs' and class members' information on the black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Personal Information; and

e. loss of privacy.

63. Plaintiffs and the class have also suffered, for example:

a. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

b. ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market; and

c. overpayments to Starwood or Marriott for products and services purchased during the Data Breach in that a portion of the price paid was for the costs of reasonable and adequate safeguards and security measures that would protect Plaintiffs' and class members' Personal Information, which Starwood and Marriott did not implement and, as a result, Plaintiffs and class members did not receive what they paid for and were overcharged by Starwood or Marriott.

64. Marriott continues to hold Personal Information of consumers, including Plaintiffs and class members.

65. Marriott has demonstrated an inability to prevent a data breach or stop it from continuing after being detected. Thus, Plaintiffs and class members have an interest in ensuring that their Personal Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

66. Pursuant to Practice Book §§ 9-7, 9-8, and 9-9, Plaintiffs bring this lawsuit on behalf of themselves and as a class action on behalf of the following class:

> **All U.S. citizens who are domiciled abroad and whose Personal Information was compromised, accessed, or stolen in the Data Breach**

No member of this class satisfies the minimal diversity requirement of the Class Action Fairness Act, 28 U.S.C. § 1332(d), because it consists entirely of American citizens domiciled abroad who thus are not citizens of any U.S. state for purposes of 28 U.S.C. § 1332.

67. Excluded from the class are: Defendants; any entities in which any Defendant or Defendants' subsidiaries or affiliates have a controlling interest; Defendants' officers, agents, and employees; and Defendants' immediate family members. Also excluded from the class are judges and court personnel in this case, and any member of their immediate families.

68. Plaintiffs reserve the right to: (i) introduce sub-classes, and (ii) expand, limit, modify or amend class or sub-class definitions.

69. **Numerosity and Ascertainability. Practice Book § 9-7(1).** The members of the class are ascertainable and are so numerous that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiffs at this time, Marriott has acknowledged that Personal Information of hundreds of millions of customers all over the world has been compromised.

70. **Commonality and Predominance. Practice Book §§ 9-7(2) and 9-8(3).** This action involves common questions of law or fact that predominate over any questions affecting individual class members, including:

i. whether Defendants failed to comply with internal company policies and applicable laws, regulations, and industry standards relating to data security;

ii. whether Defendants knew or should have known that Starwood or Marriott did not employ reasonable measures to keep Plaintiffs' and class members' Personal Information secure and prevent the loss or misuse of that information;

iii. whether Defendants owed a legal duty to Plaintiffs and class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

iv. whether Defendants breached a legal duty to Plaintiffs and class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

v. whether class members' Personal Information was accessed, compromised, or stolen in the Data Breach;

vi. whether Defendants knew about, or should have known about, the Data Breach before it was announced to the public in September 2018;

vii. whether Defendants failed to timely notify the public of the Data Breach;

viii. whether Plaintiffs and the class members are entitled to actual, statutory, or other forms of monetary relief; and

ix. whether Plaintiffs and the class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

71. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the common questions that predominate.

72. **Issue Classes. Practice Book § 9-9(4).** In the unlikely event a particular issue is not amenable to classwide adjudication, the predominance of common questions among the remaining issues supports class certification on those issues pursuant to Practice Book § 9-9(4).

73. **Typicality. Practice Book § 9-7(3).** Plaintiffs' claims are typical of the claims of the other class members because, among other things, Plaintiffs and the other class members were injured through Defendants' misconduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other class members, which arise from the same facts, and there are no defenses that are unique to Plaintiffs.

74. **Adequacy of Representation. Practice Book § 9-7(4).** Plaintiffs will fairly and adequately represent and protect the interests of the members of the class. Plaintiffs' counsel are competent and experienced in litigating complex class actions. Plaintiffs and their counsel will fairly and adequately protect class members' interests.

75. **Superiority of Class Action. Practice Book § 9-8(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the class is impracticable. Furthermore, the adjudication of this controversy through this class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied.

76. **Declaratory and Injunctive Relief. Practice Book §§ 9-8(1) and 9-8(2).** The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other class members and otherwise impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS ALLEGED ON BEHALF OF THE CLASS

COUNT ONE: NEGLIGENCE, AGAINST ALL DEFENDANTS

77. Plaintiffs repeat and reallege paragraphs 1-76, as if fully set forth herein.

78. Defendants owed a duty to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in Starwood's or Marriott's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things: (a) designing, maintaining, and testing security systems to ensure that Plaintiffs' and class members' Personal Information in Starwood's or Marriott's possession was adequately secured and protected; (b) implementing processes that would timely detect a breach of Starwood's or Marriott's security system; (c) timely acting upon warnings and alerts, including those generated by Starwood's or Marriott's own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

79. By knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to Plaintiffs' and class members' Personal Information, Defendants breached their duty to Plaintiffs and class members to adequately protect and safeguard Personal Information. Further, Defendants failed to provide adequate oversight of Personal Information with which they were entrusted, resulting in the Data Breach.

80. Defendants should have discovered the Data Breach prior to September 2018. Defendants knew or should have known about the Data Breach prior to that time based, for example, on Marriott's due diligence in acquiring Starwood in 2016.

81. Furthermore, the law imposes an affirmative duty on Defendants to timely disclose unauthorized access and theft of Personal Information to Plaintiffs and class members, so they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of Personal Information.

82. Defendants breached their duty to notify Plaintiffs and class members of the unauthorized access by failing to notify Plaintiffs and class members of the Data Breach until November 30, 2018, months after the Data Breach was purportedly discovered, and four years since the Data Breach commenced. Defendant Marriott has not provided sufficient information to Plaintiffs and class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and class members.

83. Defendants' failure to implement proper security measures to protect Plaintiffs' and class members' Personal Information, as well as Defendants' failure to timely notify Plaintiff and class members of the Data Breach, have caused Plaintiffs and class members to suffer injury and damages.

84. But for Defendants' negligent breach of their duties owed to Plaintiffs and class members, their Personal Information would not have been accessed stolen, or compromised.

85. As a direct and proximate result of Defendants' negligence, Plaintiffs and class members have been injured as described herein, and are entitled to damages,

including punitive damages, in an amount to be proven at trial. Plaintiffs' and class members' injuries include, for example:

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds;

f. costs associated with inability to obtain money from their financial accounts or being limited in the amount of money they were permitted to obtain from their financial accounts, including missed payments on bills and loans, and late charges and fees;

g. adverse effects on their credit, including lowered credit scores resulting from credit inquiries following fraudulent activities;

h. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing payment cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing

withdrawal and purchase limits on compromised accounts, and replacing passports;

i. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;

j. damages to and diminution in the value of their Personal Information entrusted, directly or indirectly, to Defendants;

k. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Marriott's possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and class members' Personal Information; and

l. overpayment for Defendant's services because Plaintiffs and class members did not get the protection of their Personal Information for which they bargained.

COUNT TWO: NEGLIGENCE *PER SE*, AGAINST ALL DEFENDANTS

86. Plaintiffs repeat and reallege paragraphs 1-85, as if fully set forth herein.

87. Defendants owed a duty to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in Marriott's or Starwood's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things: (a) designing, maintaining, and testing

security systems to ensure that Plaintiffs' and class members' Personal Information in Starwood's or Marriott's possession was adequately secured and protected; (b) implementing processes that would timely detect a breach of Starwood's or Marriott's security systems; (c) timely acting upon warnings and alerts, including those generated by Starwood's or Marriott's own security systems; and (d) maintaining data security measures consistent with industry standards.

88. Defendants should have discovered the Data Breach prior to September 2018. Defendants knew or should have known about the Data Breach prior to that time based, for example, on Marriott's due diligence in acquiring Starwood in 2016.

89. Furthermore, the law imposes an affirmative duty on Defendants to timely disclose unauthorized access and theft of Personal Information to Plaintiffs and class members, so they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of Personal Information.

90. Defendants breached their duty to notify Plaintiffs and class members of the unauthorized access by failing to notify Plaintiffs and class members of the Data Breach until November 30, 2018, months after the Data Breach was purportedly discovered, and four years after the Data Breach commenced. Defendant Marriott has not provided sufficient information to Plaintiffs and class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and class members.

91. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses such as Starwood and Marriott of failing to use reasonable

measures to protect Personal Information. FTC publications and orders, including those described above, also form part of the basis of Defendants' duty in this regard.

92. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information, failing to comply with applicable industry standards, and by failing to timely notify Plaintiff and class members of the Data Breach. Defendants' conduct was particularly egregious given the nature and amount of Personal Information Starwood and Marriott obtained and stored (pertaining to approximately 383 million unique records), and the foreseeable consequences of a data breach at hospitality chains as large as Starwood and Marriott, including, specifically, the damages that would result to Plaintiffs and class members.

93. Defendants' violation of the FTC Act constitutes negligence *per se*.

94. Plaintiffs and class members are within the class of persons that the FTC Act was intended to protect.

95. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices pertaining to Personal Information, caused the same or similar harm as that suffered by Plaintiffs and the class.

96. But for Defendants' breach of duties owed to Plaintiffs and class members, Plaintiffs and class members would not have been injured.

97. The damages suffered by Plaintiffs and class members were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to fulfill their duties, and that the breach would cause Plaintiffs and class members to experience the foreseeable harms associated with exposure of their Personal Information.

98. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the class have suffered, and continue to suffer, injury which they could not reasonably avoid, including ascertainable losses of money or property, and other damages as alleged above.

99. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and class members have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Marriott's possession and is subject to further unauthorized disclosures so long as Marriott fails to undertake appropriate and adequate measures to protect it.

COUNT THREE: BREACH OF IMPLIED CONTRACT, AGAINST ALL DEFENDANTS

100. Plaintiffs repeat and reallege paragraphs 1-99, as if fully set forth herein.

101. Defendants solicited Plaintiffs and class members to become loyalty program members and/or to make reservations at Starwood or Marriott properties. Plaintiffs and class members accepted Defendants' offers and became loyalty program members and/or made such reservations.

102. When Plaintiffs and class members became loyalty program members or made reservations with Starwood or Marriott, they were required to—and did—

provide their Personal Information to Defendants. In so doing, Plaintiffs and class members entered into implied contracts with Starwood or Marriott pursuant to which Defendants agreed to protect such Personal Information and to timely and accurately notify Plaintiffs and class members if their Personal Information had been accessed, stolen, or compromised.

103. Each reservation by Plaintiffs and class members was made pursuant to mutually agreed-upon implied contracts with Starwood or Marriott under which Defendants agreed to safeguard and protect Plaintiffs' and class members' Personal Information and to provide accurate and timely notice if such information was accessed, stolen, or compromised.

104. Plaintiffs and class members would not have provided their Personal Information to Defendants in the absence of such an implied contract.

105. Plaintiffs and class members fully performed their obligations under the implied contracts with Starwood or Marriott.

106. Defendants breached the implied contracts they made with Plaintiffs and class members by failing to safeguard or protect class members' Personal Information and by failing to provide accurate and timely notice when their Personal Information was accessed, stolen, or compromised.

107. As a direct and proximate result of Defendants' breaches of the implied contracts alleged above, Plaintiffs and class members sustained actual losses and damages as described herein and paid more than they otherwise would have paid for Marriott's or Starwood's services.

COUNT FOUR:
BREACH OF THE DUTY OF GOOD FAITH AND FAIR DEALING, AGAINST ALL DEFENDANTS

108. Plaintiffs repeat and reallege paragraphs 1-107, as if fully set forth herein.

109. Common law implies a covenant of good faith and fair dealing in every contract. Plaintiffs and class members contracted with Starwood or Marriott by accepting offers to stay at one or more hotels.

110. Plaintiffs and class members performed the duties and obligations required under their agreements with Starwood or Marriott.

111. All conditions precedent required for Starwood's or Marriott's performance under their contracts with Plaintiffs and class members have occurred.

112. Defendants did not provide, unfairly interfered with, or frustrated the right of, Plaintiffs and class members to receive the full benefits of their agreements with Starwood or Marriott.

113. Plaintiffs and class members were damaged by Defendants' breach in that they paid for, but did not receive, the protections for their Personal Information to which they were entitled under the contracts with Starwood or Marriott.

COUNT FIVE:
CONNECTICUT UNFAIR TRADE PRACTICES ACT, C.G.S. § 42-110b, AGAINST ALL DEFENDANTS

114. Plaintiffs repeat and reallege paragraphs 1-113, as if fully set forth herein.

115. Defendants engaged in the conduct alleged in this Complaint in the context of transactions intended to result in, and which did result in, the sale of room reservations at Defendants' hotels to Plaintiffs and class members.

116. Both before and after its acquisition by Marriott, Starwood's principal place of business and corporate headquarters was in Stamford, Connecticut. Starwood thus operated a trade or commerce intimately associated with Connecticut.

117. Defendants' acts and omissions which led to the Data Breach, including but not limited to their inadequate data security measures and failure to properly protect consumers' Personal Information, originated from and was effectuated in Connecticut, as Marriott maintains its Starwood data warehouse, which stored Plaintiffs and the class members' Personal Information, in or about Stamford, Connecticut. For this reason, Plaintiffs and class members suffered their injury, the theft of their Personal Information, in Connecticut.

118. Defendants Starwood and Marriott are "persons" as defined by C.G.S § 42-110a(3).

119. Defendants Starwood and Marriot are engaged in "trade" or "commerce" as those terms are defined by C.G.S. § 42-110a(4).

120. At the time of filing this Complaint, Plaintiffs are sending notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S. § 42-110g(c). Plaintiffs will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

121. As alleged above, Defendants engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of C.G.S. § 42-110b, including:

a. representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. representing that services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

122. Defendants made misrepresentations and omissions relating to Personal Information, data security, and the Data Breach that were material because they were likely to deceive reasonable consumers.

123. Defendants made misrepresentations and omissions relating to Personal Information, data security, and the Data Breach that were intended to mislead Plaintiffs and class members and induce them to rely on their misrepresentations and omissions.

124. Had Defendants disclosed to Plaintiffs and class members that Starwood's or Marriott's data systems were not secure and, thus, were vulnerable to attack, Defendants would have been required to implement and adopt reasonable data security measures to comply with their legal obligations, and would have been forced to disclose material information regarding security. Instead, without any such disclosure, Defendants maintained customer Personal Information in Starwood's or Marriott's databases and networks, where it was insecure and subject to attack for four years.

125. Customers, including Plaintiffs and class members, would not have provided Starwood or Marriott with their Personal Information had they known that Starwood or Marriott was misrepresenting the security of, and omitting the

flaws in, its databases. Consumers, including Plaintiff and class members, would have been less likely to book hotel reservations with Starwood or Marriott had Defendants disclosed the truth about Starwood's and Marriott's lax security. Additionally, Starwood's and Marriott's rooms would have been worth less to Plaintiffs and class members if the truth had been known in the marketplace that Starwood and Marriott employed inadequate security measures.

126. Defendants' unlawful, deceptive, and unconscionable acts include:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and class members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' Personal Information;

d. misrepresenting that they would protect the confidentiality of Plaintiffs' and class members' Personal Information, including by implementing and maintaining reasonable security measures;

e. misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' Personal Information;

f. omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and class members' Personal Information;

g. omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' Personal Information;

h. continuing to accept credit and debit card payments, and continuing to store other Personal Information, after they knew or should have known of the Data Breach and before they purportedly remediated the Breach; and

i. failing to timely notify Plaintiffs and class members of the Data Breach.

127. These unfair acts and practices violated duties imposed by law, including but not limited to the FTC Act. Specifically, Defendants violated Section 5 of the FTC Act, 15 U.S.C. § 45, through their failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data.

128. Defendants' conduct was intentional, knowing, and/or malicious because they knew or were reckless in not knowing the value of consumers' Personal Information, and that databases containing such information were targets for

hackers, yet they did not take adequate measures to secure their databases from hacking.

129. Defendants' violations of Connecticut law were done with reckless indifference to the rights of Plaintiffs and class members or, were an intentional or wanton violation of those rights.

130. Defendants' unfair acts and practices were: (i) ongoing failures to secure the Personal Information of class members; and (ii) ongoing failures to comply with common law and statutory duties pertaining to the security of such Personal Information. Such ongoing failures continued at least until the announcement of the Data Breach in November 2018. This action is filed within three years of the alleged violations, pursuant to C.G.S. 42-110g(f).

131. Plaintiffs and class members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

132. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and class members have suffered and will continue to suffer injury which they could not reasonably avoid, including ascertainable losses of money or property, and other damages as alleged above.

COUNT SIX: C.G.S. § 42-471, PROTECTION OF SOCIAL SECURITY NUMBERS AND PERSONAL INFORMATION, AGAINST ALL DEFENDANTS

133. Plaintiffs repeat and reallege paragraphs 1-132, as if fully set forth herein.

134. Connecticut law provides, in relevant part, that "[a]ny person in possession of personal information of another person shall safeguard the data, computer files

and documents containing the information from misuse by third parties." C.G.S. 42-471(a). As defined in this statute, "personal information" means "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, ... an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number." C.G.S. 42-471(c).

135. As alleged in detail above, Defendants did not "safeguard ... from misuse by third parties" uniquely-identifying Personal Information including but not limited to credit card numbers, debit card numbers, passport numbers, and other government-issued identification data. Defendants failed to institute reasonable safeguards to prevent the Data Breach and failed to disclose the Data Breach despite knowing of its existence for at least the period between September 8 and November 30, 2018. Failure to disclose constitutes a distinct failure to "safeguard the data ... from misuse by third parties" inasmuch as it prevented Plaintiffs and class members from taking timely remedial measures to tamp down "misuse."

136. As a direct and proximate result of Defendants' violations of C.G.S. § 42-471, Plaintiffs and class members have suffered and will continue to suffer injury which they could not reasonably avoid, including ascertainable losses of money or property, and other damages as alleged above.

137. In addition, Plaintiffs and the class assert claims for civil penalties to the maximum extent provided for under C.G.S. § 42-471(e) and C.G.S. § 42-472.

PRAYER FOR RELIEF

Plaintiffs, both individually and on behalf of class members, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. Certify this action as a class action, proper and maintainable pursuant to Practice Book §§ 9-7 and 9-8;
2. Declare that Plaintiffs are proper class representatives;
3. Appoint the undersigned as class counsel;
4. Grant permanent injunctive relief prohibiting Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;
5. Require Defendants to provide appropriate credit monitoring services to Plaintiffs and the class;
6. Award Plaintiffs and class members compensatory, consequential, and general damages in an amount to be determined at trial;
7. Order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;
8. Award statutory damages, treble damages, and punitive or exemplary damages, to the extent permitted by law;
9. Award Plaintiffs reasonable attorneys' fees, costs, and expenses pursuant to C.G.S. § 42-110g;
10. Award prejudgment and post-judgment interest at the maximum legal rate; and
11. Grant all such other relief as the Court deems just and proper.

Dated at Greenwich, Connecticut this 7th day of May, 2019

IVEY, BARNUM & O'MARA LLC

/s/ Michael J. Jones
Michael J. Jones
170 Mason Street
Greenwich, Connecticut 06830
Telephone: (203) 661-9462
mjones@ibolaw.com

PIERCE BAINBRIDGE BECK PRICE & HECHT LLP

Deborah H. Renner (*PHV* pending)
William L. Geraci (*PHV* pending)
277 Park Avenue, 45th Floor
New York, New York 10172
Telephone: (212) 484-9866
drenner@piercebainbridge.com
wgeraci@piercebainbridge.com

Thomas D. Warren (*PHV* pending)
355 S. Grand Ave., 44th Floor
Los Angeles, California 90071
Telephone: (213) 262-9333
twarren@piercebainbridge.com

Theodore J. Folkman (*PHV* pending)
One Liberty Square
Boston, Massachusetts 02109
Telephone: (617) 313-7401
tfolkman@piercebainbridge.com

Attorneys for Plaintiffs
Aryeh and Sassya Simon